Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 08 June 2004

Daily Overview

- The South Florida Sun−Sentinel reports Delray Beach police said three men found pawing through post office trash bins were paid recruits in an identity theft and credit fraud ring; more arrests are anticipated. (See item 16)

- The Department of Homeland Security has designated all of the activities for former President Ronald Reagan's Memorial Service as a National Special Security Event; federal resources will be deployed to maintain the level of security needed for the event and the area. (See item 30)

- IDG News Service reports anti−virus software companies are warning customers about a new e−mail worm that targets unpatched Microsoft Windows machines with either of two recently disclosed software vulnerabilities. (See item 32)

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical Industry and Hazardous Materials**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information Technology and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

Current Electricity Sector Threat Alert Levels: <u>Physical</u>: Elevated, <u>Cyber</u>: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) – http://esisac.com]

1. *June 07, Reuters* — **NYMEX crude ends up as gasoline rises on glitch.** NYMEX crude oil futures ended modestly higher on Monday, June 7, on the back of gasoline's rise amid talk of a glitch in a Mississippi refinery. The day's gains stemmed a three−session loss. However, the advance was tempered as the market remained under pressure after last week's OPEC decision to increase production quotas. **NYMEX gasoline rose amid talk that a fluid catalytic**

cracking unit at the ChevronTexaco refinery in Pascagoula, MS, was down. Company officials refused to comment on the issue, saying it was a market−related matter. **The refinery has a crude distillation capacity of about 350,000 barrels per day and a cat−cracking cap of about 70,000 bpd.**
Source: http://biz.yahoo.com/rc/040607/markets_energy_nymex_2.html

2. *June 06, New York Times* — **Nuclear power plant in New York prepares to drill for terror attack.** For two decades, the emergency drills at the Indian Point nuclear reactors in New York have been meant to show federal regulators how plant operators and local public safety officials would cope with a radiation release that began with a pipe break or a pump failure. However, the exercise planned for Tuesday, June 8, has a different script and a different audience. The hypothetical crisis that will be the subject of the drill is a terrorist attack. This time, the targets of persuasion are not only the Nuclear Regulatory Commission and the Federal Emergency Management Agency, but also the local governments and the public. **The terrorism scenario is a first for an emergency drill at Indian Point, the nuclear plant closest to ground zero and the nexus of much anxiety since the September 11 attacks.** Among the differences in this exercise is the participation of the F.B.I., said a spokesperson for Entergy, which owns Indian Point, in Westchester County.
Source: http://www.nytimes.com/2004/06/06/nyregion/06indianpoint.html?ex=1087099200&en=9532e23ea2817263&ei=5062

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 07, The Intelligencer (Wheeling, WV)* — **Hazardous materials flow study to begin. Knowing exactly what hazardous materials are being transported through a community is the key to forming a safety plan in the event of a spill or leak.** The Buckhannon, WV, firm of R.D. Zande & Associates will conduct a study of hazardous materials commodity flow in Marshall and Wetzel counties June 7 through Friday, June 11. The purpose of the study, the first phase two−part project funded by the Marshall−Wetzel Local Emergency Planning Committee, **is to collect data including the identifications of what hazardous commodities are being transported through the counties at various time intervals. These findings will be used to develop a new hazardous materials response plan.** "The hazardous materials (response) plan was last updated in 1999," said Marshall County Office of Emergency Services Director, Thomas D. Hart. "That was also the last time a commodity flow study was conducted for both counties." **According to a news release from the Marshall County OES, all transportation and transmission systems capable of carrying hazardous materials will be analyzed. Highways, railways, waterways and pipelines are some examples.**
Source: http://news−register.net/community/story/067202004_com02.asp

[Return to top]

Defense Industrial Base Sector

4.

June 07, Reuters — **U.S. plans to cut troops in South Korea. The United States plans to cut its troops in South Korea by a third by the end of next year, part of a worldwide shift to use of higher technology in defense, the two countries said Monday, June 7. "U.S. officials told us last night that under their Global Defense Posture Review they are planning to reduce the number of U.S. troops here by 12,500 by the end of December 2005,"** said Kim Sook, head of the ministry's North America bureau. That would include 3,600 U.S. soldiers already earmarked for deployment to Iraq from South Korea. A statement released by United States Forces Korea (USFK) confirmed the details of the proposed redeployment plan. Washington announced late last year that it aimed to transform its forces deployed worldwide using advances in military technology and smaller more mobile units to better respond to different types of security needs. The United States has earmarked $11 billion for force upgrades, while South Korea has discussed plans to increase defense spending. Because the 1950–53 Korean War ended in a truce rather than a peace treaty, the two Koreas are technically still at war.
Source: http://abcnews.go.com/wire/US/reuters20040607_51.html

5. *June 05, The Sun (WA)* — **Navy ships, subs now under one command.** Naval Base Kitsap in Washington became a reality Friday, June 4, as the Bremerton and Bangor installations were merged into one command at a ceremony. **The Navy is hoping to save more than $1 million by consolidating the base operating services at the now defunct Naval Station Bremerton and Naval Submarine Base Bangor. The consolidated base will be responsible for the homeporting of four surface ships, including an aircraft carrier, nine Trident submarines and one fast–attack research sub.** Naval Base Kitsap, first conceived nearly two years ago, is the first consolidation of major ship and submarine bases. The merger of Bremerton and Bangor is one of four similar base consolidations the Navy has undertaken. It's part of the Navy's overall effort to save money in every area in order to build more ships and aircraft over the next four years.
Source: http://www.thesunlink.com/redesign/2004–06–05/local/20040605_004.shtml

6. *June 04, General Accounting Office* — **GAO–04–349: Military Aircraft: DoD Needs to Determine Its Aerial Refueling Aircraft Requirements (Report).** With the heavy pace of operations in support of the war on terrorism, the Department of Defense (DoD) and the Air Force have become increasingly concerned about their aging aerial refueling aircraft. General Accounting Office (GAO) last reviewed the aerial refueling fleet in 1996 and found that KC–135 aircraft were aging and becoming increasingly costly to maintain and operate. In December 2001, we began new work on the Air Force's requirements for refueling aircraft. **GAO was asked to review (1) the extent to which the current fleet has met aerial refueling needs, and the cost and effort to operate and sustain the fleet, (2) DoD's current refueling requirements, and (3) options to meet future aerial refueling needs.** We recommend that the Secretary of Defense (1) conduct a study to determine the current and projected aerial refueling requirements, and (2) direct that the planned analysis of alternatives be a comprehensive study of all reasonably available options or options currently being tested, including using contractor–provided aerial refueling services. DoD concurred with each recommendation.
Source: http://www.gao.gov/new.items/d04349.pdf

[Return to top]

Banking and Finance Sector

7. *June 07, IDG News Service* — **Man pleads guilty to wireless hack into stores.** A Michigan man pleaded guilty on Friday, June 4, to four counts of wire fraud and unauthorized access to a computer after he and two accomplices used a vulnerable wireless network at a Lowe's Companies Inc. store in Michigan to attempt to steal credit card numbers from the company's main computer systems in North Carolina and other Lowe's stores in the U.S. **The case stems from a series of hacks in October and November 2003 in which the two accomplices discovered a loosely protected wireless local area network connection at a Lowe's store in Southfield, MI, while scanning for open connections, or "war driving" in the area.** The trio subsequently used the open access point to compromise the entire corporate network of the North Carolina–based home improvement store company, hacking into stores in California, Kansas, South Dakota and other states in the weeks that followed. **Among other things, the three attempted to install a modified version of a credit processing program called "tcpcredit" that skimmed credit account information for every transaction processed at a particular Lowe's store,** according to the indictment files with the U.S. District Court for the Western District of North Carolina.
Source: http://www.infoworld.com/article/04/06/07/HNwirelesshack_1.h tml

8. *June 07, Canadian Press* — **Canada–U.S. money–laundering, drug sweep. Police have laid almost 160 charges in a cross–border money–laundering and drug–trafficking ring. Two dozen people have been charged in the year–long investigation,** police said Monday, June 7. "We've arrested, or we're in the midst of arresting, people throughout the Toronto, Windsor and Detroit areas for grow op and money laundering," said Michele Paradis, spokesperson for the Royal Canadian Mounted Police. Some 50 marijuana grow operations were raided overnight in the three cities. The sweep is in conjunction with the U.S. Drug Enforcement Agency and Michigan State Police, Paradis said.
Source: http://cnews.canoe.ca/CNEWS/Canada/2004/06/07/pf–489567.html

[Return to top]

Transportation Sector

9. *June 07, The Trucker* — **Con–Way forming new company. Con–Way Transportation Services Inc. is forming a new company, Con–way Truckload (CTL). CTL is to start operating during the first quarter of 2005, according to a company news release.** Gerald L. Detter, president and CEO, said CTL will serve Con–Way's three regional less–than–truckload carriers: Con–Way Central Express, Con–Way Southern Express and Con–Way Western Express. He said CTL will assist the three regional offices by providing linehaul service on full loads of LTL shipments moving in transcontinental traffic lanes. Douglas W. Stotlar, executive vice president and chief operating officer, said CTL "will be free–standing with its own employees and equipment. In its first two years of business our plan is to add approximately 450 new ... jobs to Con–Way's existing workforce of more than 18,500 employees. All drivers will be company employees with contract drivers utilized as needed." CTL will service transcontinental routes in addition to the company's existing truckload providers. Con–Way has trucking operations throughout the United States, Canada and Mexico with revenue of $2.2

billion.
Source: http://www.thetrucker.com/stories/06_04/0607_new_co.html

10. *June 07, Associated Press* — **Amtrak train searched after report. An Amtrak train on its way to Washington was stopped and searched Sunday, June 6, in western Maryland after U.S. military personnel on board reported suspicious activity by two men, officials said.** Barry Maddox, an FBI spokesman, said the agency had found no cause for alarm. No charges were filed against the men, who weren't identified by name or nationality, Maddox said. The two men were questioned and released Sunday night, Amtrak spokesman Dan Stessel said, with law enforcement officials deeming "them no longer of interest." Deputy State Fire Marshal W. Faron Taylor said the military personnel on the train noticed "suspicious activity" from the men. Taylor said one of the men appeared to have an object concealed beneath his clothing. About 200 people were ordered off the train, Taylor said. He said no explosives were found. Stessel said trains are stopped because of similar reports about once a week, although passengers are not usually detained.
Source: http://www.newsday.com/news/nationworld/nation/sns−ap−brf−tr ain−stopped,0,3302622.story?coll=ny−nationalnews−headlines

11. *June 07, News 14 Carolina* — **Security intensifies on Amtrak routes. Security was beefed up on some of the nation's rail routes Monday, June 7, including one that stops in Charlotte, NC. Transportation Security Administration (TSA) workers began screening checked bags Monday on Amtrak's five long−distance trains that leave Washington, DC's Union Station each weekday. Screeners will use X−ray machines, bomb sniffing dogs and wands that can detect traces of explosives.** Security on railways has heightened after the March 11 railway bombing in Madrid, Spain. Easy access to trains and train platforms make them vulnerable to terrorist attacks, security officials say. TSA officials say it is crucial to preventing fatal terror attacks like the one that killed nearly 200 people in Spain three months ago. The agency said it is testing the waters by beginning the second phase of its Transit and Rail Inspection Pilot. The first phase began Monday with passenger screening. In the second phase, bags will be screened for explosives. Officials are hoping that the new protocol will be successful enough to catch on across the country. The pilot screenings will continue through June 30. If they are successful, TSA said the new check−in policies could be adopted at train stations nationwide.
Source: http://www.news14charlotte.com/content/local_news/?ArID=6531 2&SecID=2

12. *June 07, Bloomberg* — **Mexican trucks may ship to U.S. cities, Supreme Court says.** The U.S. Supreme Court cleared the way for Mexican trucks to carry goods to destinations across the U.S., allowing the Bush administration to boost cross− border trade by canceling a ban that was in place since 1982. **The unanimous decision lets President George W. Bush restore provisions of the North American Free Trade Agreement that former President Bill Clinton had rejected.** Labor unions and environmental groups argued an air−quality study was needed to assess the risks of allowing Mexican trucks in the U.S. U.S. manufacturers such as Whirlpool Corp. and General Electric Co. that produce on both sides of the border will benefit from the ruling, which will help cut the time and cost it takes to ship from Mexico, the U.S.'s No. 2 trading partner. Mexico and the U.S. traded $236 billion of goods last year.
Source: http://quote.bloomberg.com/apps/news?pid=10000103&sid=aOXgZH MC42iU&refer=us

13. *June 07, Associated Press* — **All clear after Southwest Airlines cargo terminal. The evacuation order has been lifted Monday, June 7, at a cargo terminal at Dallas Love Field after tests showed a package did not contain explosives. The late morning incident began when routine checks found traces of what could have been an explosive on a package.** Special dogs were brought in to check the item at the Southwest Airlines cargo facility. Officials also contacted the shipper of the package. Transportation Security Administration official Mike Restovich says Love Field is safe and the testing was a precaution. Southwest is based in Dallas.
Source: http://www.dfw.com/mld/startelegram/news/state/8862095.htm?1 c

14. *June 07, San Mateo County Times Online* — **Baby bullet train shoots out of the gate. After two years of construction, $110 million and numerous headaches for commuters, Caltrain will launch its much anticipated "baby bullet" express trains Monday, June 7.** The baby bullet promises something all too rare in an age when traffic congestion seems perpetual and the term "rush hour" is a gross understatement: a quicker commute. **The trains will shave a whopping 40 minutes off a Caltrain trip between San Francisco and San Jose. The baby bullets will make the run in just under an hour.** "I think (the baby bullet) is a significant leap, because now (Caltrain) will be competitive with the automobile," said Margaret Okuzumi, executive director of the rail–advocacy group BayRail Alliance. "I think it will attract a lot of new riders to the train, especially with gas prices this high." The launch also brings an overhaul of Caltrain's schedule, which will pump the number of trains running each day to the highest level ever. But it also mean less service for some stations that serve fewer riders. Caltrain will add 10 baby bullet trains a day to its normal schedule of 76 trains. The schedule includes two southbound morning baby bullets leaving San Francisco and two north– bound evening baby bullets leaving San Jose to accommodate riders making a reverse commute.
Source: http://www.sanmateocountytimes.com/Stories/0,1413,87~11268~2 197575,00.html

15. *June 07, Business Travel News* — **Private jet transportation cos. report soaring business.** The business jet market is booming, at least according to numerous private transportation companies that recently have reported strong sales and developed new, more flexible models. **Executives at these companies said corporate interest is driven by several factors, including the decreasing number of premium seats offered by commercial carriers, service cuts to certain smaller communities and the increasing need of corporate flight departments for supplemental lift.** "On both corporate and leisure, we are seeing a lot more business to places that are hard to reach," said Ken Austin, executive vice president at Marquis Jet, a private jet membership company affiliated with NetJets. Norwell, MA–based Sentient Jet said it has sold 1,700 memberships, roughly 60 percent of which are used for business travel. Of that 60 percent, about half is "true corporate," which involves travel managers and other corporate decision–makers. **Meanwhile, Delta AirElite Business Jets, the only business jet operator in the United States affiliated with a major commercial airline recently said that in the past year it had doubled its revenue flight hours.** Launched late last month, OneSky Network is an online portal providing users with step–by–step information for actually purchasing the services of specific charter aircraft.
Source: http://www.btnmag.com/businesstravelnews/headlines/othernews _display.jsp?vnu_content_id=1000525542

Postal and Shipping Sector

16. *June 05, South Florida Sun−Sentinel* — **Three arrested at Delray post office. Three men found pawing through post office trash bins were paid recruits in an identity theft and credit fraud ring, Delray Beach, FL, police said Friday, June 4, and more arrests are anticipated.** The trio was arrested about 12:30 a.m. Thursday, June 3, after two of them were seen going through undelivered mail in a Dumpster while the third man hid behind a column, police spokesman Jeff Messer said. **Police had been contacted by postal inspectors, who watched on surveillance cameras as the men raided the Dumpster after slipping onto the property through a hole in the fence, Messer said.** The inspectors suspected the men were picking out undeliverable mail that had been discarded, removing credit card information and blank checks issued to credit card customers. The materials could be used to set up false identities or make unauthorized purchases, according to police.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pmail05
jun05,0,7131083.story?coll=sfla−news−palm

Agriculture Sector

17. *June 06, Associated Press* — **Infection that damages wheat crops. Plant experts are predicting a widespread outbreak of wheat scab, a fungus that withers the grain and produces a chemical that can sicken humans and livestock. Wheat scab is present every year in small amounts but this year probably will cover crops from the east coast to as far west as Missouri or Arkansas,** said Erick DeWolf, assistant professor of plant pathology at Penn State University. The disease, a brown film−like covering, is already abundant in Virginia. "It is pretty bleak," said Don Hershman, extension plant pathologist for the University of Kentucky. "In fact, I just talked with the pathologist at Indiana a little while ago and he said it's bleak there. Illinois isn't good, and Ohio's starting to slide, too."
Source: http://newstribune.com/articles/2004/06/06/business/06060400_19.txt

18. *June 04, U.S. Department of Agriculture* — **USDA launches Incident Command System training.** Agriculture Secretary Ann M. Veneman Friday, June 4, announced the launch of a web−based Incident Command System (ICS) training program to enhance the Department's effectiveness in responding to a wide range of emergencies. **"This ICS training will help bolster resources to manage accidental or deliberate incidents that may threaten the U.S. food supply, critical infrastructure, or economy, Veneman said"** In 2001, Veneman directed U.S. Department of Agriculture (USDA) officials to develop a single unified management plan for all USDA emergency response and recovery activities. And in March 2003, she issued a memorandum directing Department−wide implementation of the USDA National Interagency Incident Management System (NIIMS), unifying emergency response and recovery efforts under one management system for the first time in USDA history. NIMS outlines a standard incident management structure called the Incident Command System, which includes five functional areas −− command, operations, planning, logistics, and finance/administration −− for

management of all major incidents.
Source: http://www.usda.gov/Newsroom/0221.04.html

[Return to top]

Food Sector

19. *June 07, Agence France Presse* — **China to cancel thousands of food export licenses. Nearly 6000 Chinese food companies failed to pass muster when authorities checked their hygiene standards, state media reported Sunday, June 6.** The State Certification Accreditation Administration investigated conditions at more than 11,000 food processing enterprises, and gave a passing grade to only 53 percent, China Central Television said. At about 2,400 enterprises, conditions were so appalling that officials immediately determined export licenses had to be canceled, according to the report. More than 3,000 others will get a last chance to clean up their act, as their export licenses will only be temporarily suspended, the report said. **Sub−standard food has emerged as a major public health issue in China, as reports emerge virtually every week of mass food poisonings, mostly caused by poor hygiene.**
Source: http://www.theaustralian.news.com.au/common/story_page/0,574 4,9769758%255E23289,00.html

20. *June 07, Duke University Medical Center* — **Common worm provides insights into salmonella virulence.** Using a common worm as a model, researchers from Duke University Medical Center have identified specific genes within Salmonella that give the bacteria its ability to infect host cells. **They said their findings could ultimately lead to improved drugs to prevent or treat Salmonella infections.** The researchers found four genes related to the Salmonella's "molecular syringe" that are required for the bacteria to have maximum potency in infecting the worm, known as Caenorhabditis elegans. The virulence factors −− injected into the host cells by Salmonella −− act by blunting the innate immune system of C. elegans from attacking and destroying the infecting bacteria. These findings are important, the researchers said, because the C. elegans innate immune response to Salmonella infection is quite similar to that of mammals, including humans. For this reason, the researchers said that their C elegans model can provide new genetic insights into the relationships between invading microbes and their target host cells.
Source: http://www.eurekalert.org/pub_releases/2004−06/dumc−cwp06030 4.php

21. *June 07, Food Production Daily* — **Quality meat production for safer food. U.S. Researchers are to investigate the link between livestock wellbeing and the risk of foodborne disease, a move which could have widespread implications for animal husbandry and food safety.** Scientists from the Farm Animal Behaviour and Well−Being Laboratory, part of the Agricultural Research Service (ARS) of the U.S. Department of Agriculture, will study stress indicators in livestock with a view to determining the relationship between stress and the ability of pathogenic bacteria to establish themselves in animals. Donald C. Lay, research leader and animal behaviouralist at the lab, is working on an imaging system to show the movement of Salmonella bacteria through live pigs. He and colleagues are also researching alternative housing for poultry and livestock.
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=52591

22. *June 07, Agence France Presse* — **Death toll in Kenya toxic grains crisis rises. Kenyan Health Minister Charity Ngilu said some 80 villagers have died and 180 others hospitalized in eastern Kenya for eating contaminated maize since mid–April.** "The number of people who have died because of eating contaminated maize in Eastern province has reached 80 while those currently admitted in health centers are about 180," Ngilu told Agence France Presse. **Villagers in Makueni and Kitui districts reported the first death in mid–April, after they consumed maize infected with aflatoxins, moulds that grow as a result of poorly storing grains that have not dried, Ngilu explained.** Director of Medical Services James Nyikal said the government has already sent troops to the two districts, which often suffer from food shortages, to distribute relief supplies and water. Exposure to large amounts of aflatoxin over a short period causes acute liver damage and death, while the ingestion of small amounts over a longer period can cause liver cancer, according to the health ministry.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=1507&ncid=15 07&e=1&u=/afp/20040607/hl_afp/kenya_health_food_040607174337

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *June 07, Australian* — **Spray may foil anthrax attacks. Australian and U.S. bioterrorism experts believe research by a Melbourne, Australia, based company will lead to the world's first anti–anthrax spray, which can be used to protect troops and civilians from an anthrax attack.** The spray could be inhaled up to 48 hours before an expected anthrax attack to temporarily neutralize the agent until a suitable antibiotic can be administered. Both the Australian Defense Force and the U.S. military have experienced problems with the current anti–anthrax vaccines, which have caused serious side–effects to some troops. **At present, once a victim breathes anthrax and the agent produces sufficient toxin, there is nothing that can be done to save the person's life.** Such technology, if developed successfully, could allow anthrax victims to seek medical help before symptoms develop, by which stage drugs are useless. Anthrax has been used in several acts of bioterrorism, including when a sect in Japan pumped the bacteria into a Toyko factory, and when anthrax spores were mailed to the U.S. Senate and media outlets after the September 11 attacks, killing postal workers.
Source: http://townsvillebulletin.news.com.au/common/story_page/0,70 34,9765758%255E421,00.html

24. *June 07, U.S. Centers for Disease Control and Prevention* — **New test for anthrax. A new test funded by the U.S. Centers for Disease Control and Prevention (CDC) and developed in collaboration with a commercial partner has become the first test approved by the Food and Drug Administration (FDA) for detecting antibodies to anthrax.** The test

provides an easy–to–use clinical laboratory tool for assessing whether patients have been infected with anthrax. The Anthrax Quick ELISA test, which was recently approved by the FDA, detects antibodies produced during infection with Bacillus anthracis –– the bacteria that causes anthrax. The new test helps confirm a diagnosis of anthrax because it demonstrates that a person's immune system has responded to a protein produced by the infecting bacteria. **Before FDA approval of the new test, few laboratories other than the CDC and the U.S. Army had the ability to test blood for antibodies to anthrax. The new test will be available shortly for use in state and private laboratories.**
Source: http://www.cdc.gov/od/oc/media/pressrel/r040607.htm

25. *June 07, ABC News (Australia)* — **Superbug raises antibiotic fears. Normally a harmless bacterium, golden staph is carried on the skin of 50 percent of the population.** It can cause serious infections like pneumonia or septicaemia, with outbreaks in hospitals sometimes quickly spreading between patients. **But in this case, one man has died and 50 others have been infected by an antibiotic resistant strain that appears to be spreading outside hospitals in south–eastern Queensland and northern New South Wales, Australia.** Michael Whitby, the director of Infection Management Services at Brisbane's Princess Alexandra Hospital, says the organism is resistant to one particular antibiotic. "Dicloxacillin, flucloxacillin, which is a common antibiotic to treat staph infections and for that reason it is important," Whitby said. "But it's not in any way untreatable. He says although it the organism is treatable, it is concerning that it has developed resistance to common antibiotics." Antibiotics have been in use so long and in such vast quantities that some have become less effective in treating golden staph infections.
Source: http://www.abc.net.au/news/indepth/featureitems/s1126576.htm

26. *June 06, Associated Press* — **Ohio hospitals join in early warning system.** Hospitals in Ohio are joining with others to watch for signs of a terrorist attack, a move health officials say could play a vital role in early detection. **Some Cincinnati and Columbus health care centers will send information about emergency room patients to the University of Pittsburgh, where computers will monitor surges in rashes, respiratory illnesses, and other symptoms that could signal a biological or chemical attack.** Other hospitals around the state also are expected to join with the help of $330,000 in federal money. A similar early warning system was in place in Utah during the 2002 Winter Olympics. About 100 metropolitan areas around the country have some sort of detection plan, said Dr. Tracee Treadwell, chief epidemiologist with the bioterrorism preparedness and response program at the U.S. Centers for Disease Control and Prevention.
Source: http://www.thesandiegochannel.com/health/3387840/detail.html

27. *June 04, Princeton University* — **Device sorts microscopic particles with speed and precision.** In a collaboration between engineers, physicists, and biologists, Princeton scientists have invented a device that rapidly sorts microscopic particles into extremely fine gradations of sizes, opening a range of potential uses. The researchers have used the device to sort particles ranging in size from bacterial cells to large segments of DNA. **The technology could greatly accelerate the work of sequencing genomes and could find uses in many other areas, from improving the performance of pharmaceuticals to detecting bioterrorism agents.** Until now there was no way to sort large quantities of molecules or cells by size with such speed and precision, according to the researchers. Current methods separate particles only according to

major differences in size and, for particles such as DNA, can take hours to perform. The Princeton invention can distinguish large quantities of particles that are one micrometer from others that are 1.005 microns in a matter of seconds. The device consists of an array of microscopic pillars etched into silicon. Air from a syringe or other pump forces a liquid suspension of particles through the pillar array, which guides the particles into different paths. When the particles emerge from the array, they have been sorted into any number of "channels" according to size.
Source: http://www.eurekalert.org/pub_releases/2004−06/pu−ttd060404.php

[Return to top]

Government Sector

28. *June 04, Government Technology* — **Delaware Senate confirms new Homeland Security Director. David B. Mitchell was sworn in as the new Secretary of Public Safety and Homeland Security on Wednesday, June 4, immediately following his confirmation by the state Senate.** Mitchell, 53, served as superintendent of the Maryland State Police, the seventh largest state law enforcement agency in the country, with more than 2,500 employees. In that position, he was the primary law enforcement advisor to then−Gov. Parris Glendenning and a member of the governor's cabinet. After September 11, 2001, Mitchell chaired the Governor's Homeland Security Work Group, creating legislation and revising procedures and plans to better prepare and protect Maryland. He created the "Cease Fire" initiative, aimed at reducing gun crime in Maryland. Mitchell established the first statewide domestic violence and intervention and investigation team. He also implemented new initiatives in computer crimes, labor relations, DNA forensic investigations and community policing. He begins his new position immediately.
Source: http://www.govtech.net/news/news.php?id=90500

[Return to top]

Emergency Services Sector

29. *June 07, Grimsby Evening Telegraph (UK)* — **UK force ready for chemical terror attack. Specially−trained police officers are to take delivery of a nerve gas antidote to be used in the event of a terrorist attack in the UK.** Thousands of self−injecting antidote syringes will be distributed across the country, including North East Lincolnshire, to be used in a biological or chemical attack. A spokesman for the Association of Chief Police Officers (Acpo) said the distribution of such equipment should not cause panic. "Issue of the syringes to the officers concerned had been planned for some time and has already begun this year," he said. "It is not a reaction to any recent or specific threat. Humberside Police recently took part in a day−long exercise which tested officers' responses to a chemical or biological incident. It included testing decontamination procedures, working with the fire and ambulance services and command and control systems. **Although North East Lincolnshire would not be a high−profile target like London or Paris, an attack on an oil refinery or dock could be catastrophic.** The 6,000 syringes are among other specialist equipment which includes protective suits to guard against chemical, biological and radiological threats and detection and monitoring equipment.

Source: http://www.thisisgrimsby.co.uk/displayNode.jsp?nodeId=59380& command=displayContent&sourceNode=58907&contentPK=10215790

30. *June 06, Department of Homeland Security* — **Department of Homeland Security designates President Ronald Reagan Memorial Service as National Special Security Event.** The U.S. Department of Homeland Security has designated all of the activities for former President Ronald Reagan's Memorial Service as a National Special Security Event (NSSE). **A number of factors are taken into consideration when designating an event as a National Special Security Event including anticipated attendance by dignitaries and the size and significance of the event.** When an event is designated a National Special Security Event, the U.S Secret Service assumes its legally mandated role as the lead federal agency for the design and implementation of the operational security plan. Federal resources will be deployed to maintain the level of security needed for the event and the area. The Secret Service is responsible for planning, directing, and executing federal security operations at designated NSSEs and, together with state and local law enforcement partners, develops the overall security plan. In the Washington, DC area, the Metropolitan Police Department, the U.S. Capitol Police, the U.S. Park Police and a number of other federal and local agencies will play an active role in securing this event. Refer to the Fact Sheet for further details: http://www.dhs.gov/dhspublic/display?content=3703
Source: http://www.dhs.gov/dhspublic/display?content=3702

31. *June 04, Department of Homeland Security* — **Department of Homeland Security announces assistance to firefighters grants to aid America's fire departments.** Secretary Tom Ridge today, June 4, announced the first round of grants to fire departments throughout the United States in the Fiscal Year 2004 Assistance to Firefighters Grant Program. **The grants will ultimately total approximately 8,000 awards worth nearly $750 million in direct assistance to firefighters throughout the country, demonstrating Homeland Security's commitment to ensuring that America's firefighters have the resources they need to protect their communities.** "President Bush and I strongly support the critical mission of our Nation's firefighters. Through these funds, we will ensure that our Nation's emergency responders have the equipment and training they need to respond to all hazards," said Secretary Ridge. The Assistance to Firefighters Grant Program helps local fire departments purchase firefighting equipment, fund firefighter health and safety programs, enhance emergency medical services programs, and conduct fire education and prevention programs. The grants are administered by the Department's Office for Domestic Preparedness in cooperation with the Department's United States Fire Administration.
Source: http://www.dhs.gov/dhspublic/display?content=3700

[Return to top]

Information Technology and Telecommunications Sector

32. *June 07, IDG News Service* — **New worm targets old Windows flaws.** Anti−virus software companies are warning customers about a new e−mail worm that targets unpatched Microsoft Windows machines with either of two recently disclosed software vulnerabilities. The new worm, known as both "Plexus" and "Explet.A," was first detected on Wednesday and spreads by exploiting Windows machines with vulnerabilities used by two recent worms, Sasser and

Blaster, according to alerts. **Like Sasser, Plexus can exploit the recently disclosed hole in the Windows component called Local Security Authority Subsystem Service, or LSASS, which Microsoft patched in April. And, like the Blaster worm that appeared in August 2003, Plexus can also crawl through a hole in a Windows component called the DCOM (Distributed Component Object Model) interface, which handles messages sent using the RPC (remote procedure call) protocol.** Plexus spreads in files attached to e−mail messages with faked sender addresses and vague subjects such as "RE: order," "For you," and "Good offer." When users open the virus file, the worm is launched and alters the configuration of Windows so that the worm program runs each time Windows starts. It also scans the hard drive of infected computers, harvesting e−mail addresses from a variety of files, including stored Web pages written in Hypertext Markup Language. Anti−virus companies recommend that Windows users who have not done so already apply software patches for the LSASS and DCOM and update their anti−virus software.
Source: http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=3980

33. *June 07, The Register* — **Virus writers deploy bulk mail software.** Hackers have used spamming software to distribute thousands of copies of a new Trojan. **Demonize−T is a multi−stage Trojan that uses an object data exploit in Internet Explorer to download and execute an encoded visual basic script from a Website**. The Trojan then creates an executable file which appears to download a malicious program from the same website as the original script. Early analysis suggests Demonize−T is similar to previous attacks where malicious code has been used to install key loggers and password stealers. Spammers are increasingly using infected as a platform to distribute spam and this technique has come full circle with virus writers using spam to infect machines in the first place. A patch is available on the Microsoft Website: http://www.microsoft.com/technet/security/bulletin/MS03−040. mspx
Source: http://www.theregister.co.uk/2004/06/07/demonize_trojan/

34. *June 07, Federal Computer Week* — **DISA to develop IT standards.** The Defense Information Systems Agency (DISA) will oversee information technology standards for the military, according to new policy issued by Defense Department officials. As executive agent, DISA officials will identify and propose IT standards to develop and implement a standards management strategy. They will let the department carry out network−centric operations across the military and with government agencies, said the May 21 directive, "DoD Executive Agent for Information Technology Standards." DISA officials will create a plan for the department's IT shop, the Office of the Assistant Secretary of Defense for Networks and Information Integration and Chief Information Officer. The strategy will give warfighters fast, secure and easy−to−find information that will let them outsmart and outmaneuver enemy forces, according to the 11−page directive signed by Paul Wolfowitz, DOD deputy defense secretary. **The new Department of Defense IT standards policy also tells DISA to participate in industry, government and coalition forces' forums. "Facilitate the commercialization of DOD IT requirements by influencing the development of commercial standards through participation in commercial standards bodies**," the directive said.
Source: http://fcw.com/fcw/articles/2004/0607/web−disa−06−07−04.asp

35. *June 05, New Scientist* — **Passwords can sit on hard disks for years.** As people spend more time on the web and hackers become more sophisticated, the dangers of storing personal information on computers are growing by the day, security experts say. When you type in a

password, it is stored in random access memory (RAM), where it is held temporarily until other data overwrites it or the computer is switched off. But **every so often, the computer copies the contents of its RAM onto hard disk, where it is easy prey for a hacker, who can read it directly or design a worm to email it back**. The longer sensitive data stays in RAM, the more likely it is to be copied onto the disk, where it stays until it is overwritten−−which might not happen for years. Tal Garfinkel and colleagues from Stanford University have created a software tool called TaintBochs which simulates the workings of a complete computer system. Within the simulation, sensitive data can be tagged, or "tainted", and then tracked as it passes through the system. Such tracking is normally impossible on a computer. In a paper to be presented in August at the USENIX Security Conference in San Diego, CA, they conclude that **the programs took virtually no measures to limit the length of time the information is retained. Some of the tested software even copied the sensitive information, apparently without restraint.**
Source: http://www.newscientist.com/news/news.jsp?id=ns99995064

36. *June 03, Canadian Press* — **Montrealer arrested for hacking into U.S. government computer.** Royal Canadian Mounted Police (RCMP) officers have arrested a Montreal resident for hacking into a U.S. government computer. The federal force carried out the arrest on Friday, May 28, at the request of the Federal Bureau of Investigation. RCMP said in a statement Thursday, June 3, **the accused had illegally accessed a router connected to a U.S. Supreme Court warehouse and is suspected of having compromised several computers.** The man's computers have been seized and charges could be laid in the future, the RCMP said.
Source: http://cnews.canoe.ca/CNEWS/Law/2004/06/03/484817−cp.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis
Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures. **Watch Synopsis:** There is a new Worm called Plexus that exhibits many of the same characteristics that MyDoom exhibited. The initial variant does not target federal or military systems, but we can be certain that future variants may do so. This worm appears to be a blended threat and propagates by at least 5 various methods.

Current Port Attacks

Top 10 Target Ports	135 (epmap), 1026 (nterm), 1027 (icq), 445 (microsoft−ds), 9898 (dabber), 1434 (ms−sql−m), 21 (ftp), 5554 (sasser−ftp), 137 (netbios−ns), 3127 (mydoom)
	Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

Nothing to report.

[[Return to top]]

<div style="border: 2px solid blue;">

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts – Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports – The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.

</div>